USSOCOM CIO STRATEGIC PLAN 2009

UNITED STATES

SPECIAL OPERATIONS COMMAND
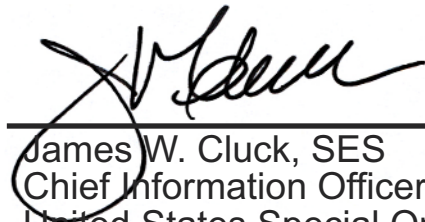
This is my vision for USSOCOM Information Technology for 2009. This plan enhances our strategy for **One Force, One Environment** and is set forth in three focus areas with near term and strategic actions to ensure the best support possible to the SOF operator. Hopefully, you will find it useful in coordinating mutual and supporting plans as we evolve the SOF Information Environment (SIE) in support of Special Operations.

James W. Cluck, SES
Chief Information Officer
United States Special Operations Command

Making a Difference

In 2008, USSOCOM deployed 30 personnel from 7 staff directorates to advise the Polish military on the activation of a Polish Special Operations Headquarters (POLSOCOM). This unprecedented outreach was the first of many collaborative sessions conducted in support of the Commander USSOCOM's International Engagement Program. To support this endeavor, USSOCOM deployed communicators from HQ USSOCOM, SOCEUR, and AFSOC with the latest SOF communications systems. Equipped with the SOF Deployable Node - Medium, a Broadband Global Area Network, and the SOF High-speed Reachback Kit, the teams provided both secure and non-secure voice, video and data to geographically separated locations for a 45 day period. This connectivity enabled senior leaders from Poland and USSOCOM to establish a partnership between both countries while demonstrating the flexibility and utility of these systems to our SOF Warriors.

I. PURPOSE

The USSOCOM Chief Information Officer (CIO) Strategic Plan defines key actions and responsibilities to evolve the SIE and take advantage of the newest technological innovations to support the SOF Operator.

II. BACKGROUND

On 4 March 2008, Admiral Eric T. Olson, the Commander, United States Special Operations Command, testified before the Senate Armed Services Committee on the Posture of Special Operations Forces. During his testimony, ADM Olson outlined three enduring priorities for Special Operations to accomplish our missions: 1) to deter, disrupt, and defeat terrorist threats to our nation 2) to develop and support our people and their families and 3) to sustain and modernize the force.

Each one of these priorities requires information technology support to ensure its success. While each priority requires varying levels of support, it is imperative that we focus our efforts to support these priorities. To aid in this goal, I identified three focus areas to direct our efforts:

- Operational Support
- Improved Business Operations
- IT Resource Management

Over the past few years we have developed, modernized, and sustained several communication platforms to include efforts to greatly expand the (SIE). The delivery of the family of systems, the Tactical LAN (TACLAN) and the Deployable/Tactical VTC have all increased the capabilities of our deployed forces.

In the next few pages, I will lay out my plan to continue to improve the support to our users. Each focus area will have near term and foundational actions that I expect us to work on as a team to move towards **One Force, One Environment.**

Ensuring (SOF) have the equipment, sensors, weapons and mobility platforms of the kind and quantity demanded by their peculiar missions requires willingness to invest in the rapid fielding of both existing solutions and cutting edge technologies.

ADM Eric T. Olson
Senate Armed Services Committee testimony, 4 Mar 08

III. AREAS FOR FOCUS

> **1. OPERATIONAL SUPPORT:** Supporting the warfighter is the ultimate priority. Advancing revolutionary, SOF-common initiatives will guarantee information interoperability on the seamless battlefield for the SOF warrior.

The USSOCOM Commander's enduring priority of "**Sustain and Modernize the Force**" requires that we continually analyze how we provide C4I operational support to Equip the Operator, Upgrade SOF Mobility and Obtain Persistent Intelligence, Surveillance and Reconnaissance Systems.

This has never been more urgent than in the age of cyber warfare in which the Joint Force Commander's conceptual battlespace is globally dynamic. At the highest levels in DoD, both culture and process are evolving with the reality that traditional geographical boundaries are null in cyberspace. SOF must evolve as well to ensure persistent global information superiority in the future operations.

With rapidly changing technology, SOF warriors require rapid technology refresh to ensure a continued advantage in the Global War on Terrorism (GWOT). The world-wide availability of low cost, high return information technology has enhanced the operational pace of our adversaries. To counter this advantage, our forces require actionable information in a rapid manner in the most remote locations. As we do not operate alone, our systems must facilitate information sharing with our interagency and multinational partners in the GWOT mission.
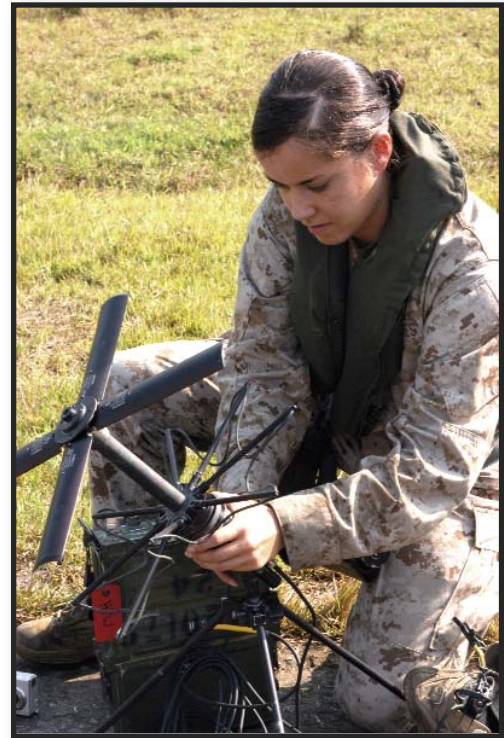
Delivery of this C4I capability means rapidly adapting current system designs and development processes to meet change head on. System interoperability, information assurance, and mission capability must be inherent in any new design. The ability to facilitate the rapid sharing of information with our current and future partners must be a first consideration in any solution, not a post-design requirement.

To sustain and modernize the force, the following near term efforts and long term foundation actions must occur.

Near-Term Actions

a. Start the transformation of the SOF Deployable Node family of terminals into modular, scalable packages to support a variety of operations. Initial fielding will consist of a mobile expeditionary capability that combines the information transport, data architecture and high capacity satellite communications into a world-wide deployable package.

b. Provide rapid technology insertion by utilizing a process of competitive prototyping. Leveraging industry research and development efforts will be essential.

c. Allow the Component Commands more flexibility in purchasing the VTC suites and computer workstations to meet their mission requirements.

d. Field two OCONUS strategically positioned communication nodes to deliver secure, interoperable, and integrated voice, video, and data service to the globally deployed SOF warrior.

e. Provide an enterprise network environment that enables evolutions in rapid synthesis of perishable data linked with decision quality tools enabling focused and actionable information at all operational levels.

Strategic Actions

a. Harness our current and emerging architecture to provide operational teams with the capability to locally store perishable data within strategic battlefield C2 nodes and use the SIE infrastructure to facilitate information sharing between strategic, operational, and tactical users regardless of location.

b. Synchronize network operations and situational awareness across the SIE through process and resource realignment, key technology insertion, and training.

c. Stand-up two geographically separate data centers for continuity of operations and as a critical step in evolving the SIE from independent networks into a global enterprise.

d. Equip the SOF operator to function anywhere in the network.

e. Field multi-functional network-ready capabilities.

f. Modernize the network to support persistent ISR.

g. Enable community of interest and cross-domain information sharing as a core capability of the network.

h. Ensure inter-agency and scalable coalition access for information sharing.

2. BUSINESS OPERATIONS: The efficiency of our workforce is facilitated by electronic tools and automation of processes to maximize productivity whether in garrison or deployed.

Directly tied to both "**Develop and support our people and their families**" and **"To sustain and modernize the force"**, business operations are focused on both improving the tools and streamlining the processes that rely on those tools. If we focus on either the tools or the people, we will not deliver the optimal solution to the user requirements.

To this end, we have created an enterprise-wide USSOCOM knowledge management team to lead this effort. While the Chief of Staff has responsibility to guide Knowledge Management for USSOCOM, it is our responsibility to relate user requirements into available technical solutions.

In addition to streamlining processes, there are many business operations improvements that require purely IT solutions. Over the past few years we have worked to improve the computing platforms at both the headquarters and within the programs of record. We have proliferated Personal Electronic Devices across the command to aid in the flow of information, just to name a few.

Within the next year, we plan to begin fielding the newest generation of Personal Electronic Devices, called the Secure Mobile Environment – Personal Electronic Device (SME-PED). Other efforts such as the consolidation of the SIPRNet domain and our Data Recovery efforts will aid in the discovery and accessibility of information across the enterprise.

However, we must plan for the continued explosion of information requirements for the user. To ensure we can access the information, we must build knowledge management solutions and leverage the newest information technology to deliver the optimal solutions to the SOF Operator. To this end, we have created a Microsoft Office Sharepoint Services 2007 (MOSS07) team within the Headquarters to plan for the migration to the newest version of our collaboration environment. We will be working with our components and Theater Special Operations Command (TSOCs) to build an architecture that will leverage SIPRNet consolidation, the Distributed Data Centers (DDCs) and MOSS07 to deliver the best collaborative environment possible.

In the dynamic and ambiguous environments that constitute today's battlefields, the ability to rapidly analyze and exploit information is key to fast sequential targeting. This requires unique skills, specialized technolgies and flexible mobility

ADM Eric T. Olson
Senate Armed Services Committee testimony, 4 Mar 08

Near-Term Actions

a. Field an initial set of Field Secure Mobile Environment – Personal Electronic Devices (SME-PED) to the enterprise.

b. Finalize the SIPRNet consolidation into a single domain for the SIE.

c. HQ USSOCOM will field Microsoft Office Sharepoint Services (MOSS 07). It is our plan to leverage SIPRNet consolidation and MOSS to provide a single collaborative environment for the enterprise. This will enhance the ability to share and discover information across the enterprise.

d. Build and implement a data strategy for Headquarters USSOCOM.

e. Finalize a USSOCOM Knowledge Management Directive outlining organizational structures, training, roles and responsibilities for KM across the enterprise.

f. Initiate an enterprise task order to provide a vehicle for all USSOCOM units to hire KM contractor support.

g. Work with the components and TSOCs to design a new Portal. Incorporate requirements for the entire enterprise including operational users.

h. Build a consolidated search capability accessible through the portal to discover data stored at the Headquarters.

Strategic Actions

a. Develop and execute a plan for a distributed data center solution.

b. Develop an architecture and solution to reduce the number of stovepiped networks and clients for our users.

c. Build a Program to fund and manage Knowledge Management from an enterprise perspective.

d. Initiate an enterprise Knowledge Management process that will identify and deliver automated solutions for business operations that will work for all users within the enterprise.

e. Implement a data strategy for the enterprise.

f. Implement a records management solution that is integrated with the portal.

3. INFORMATION TECHNOLOGY RESOURCE MANAGEMENT: As the CIO we must ensure SOF information technology (IT) investments are effectively managed to support and improve the SOF Information Environment, SOF warfighting readiness, and combat capability.

IT resource management is at the core of our responsibilities as Chief Information Officers. In the resource constrained environment we operate in today, it is difficult to ensure we effectively manage our IT investments.

As the USSOCOM CIO, we are instituting processes and investing in tools that will aid in meeting this goal. Our IT investments will be managed as portfolios and will be in compliance with the SIE.

We plan to implement an IT Portfolio Management System for the command and I am advocating its creation as a comprehensive system to synchronize the Acquisition Executive (AE), Chief Financial Officer (CFO), and my efforts to ensure all IT investments are accurately managed, authoritatively reported, and synchronized with capabilities. This system will provide visibility into how funds are being spent and whether our IT investments are contributing to the achievement of the USSOCOM mission.

In order to effectively report, defend, and manage our IT budget, we must articulate our SOF IT initiatives in terms of capability outcomes that are easily understood. Therefore, we will provide SOF commanders at all levels guidance to

ensure our budget development process for IT resources are aligned with command priorities.

Additionally, we will also ensure our major IT support contractor provides project and resourcing data required by the government and is consistent with our acquisition and financial communities.

USSOCOM continues to transform its respective capabilities in the areas of communication, information technology, automation of intelligence data and collaboration tools into a single integrated SOF environment

ADM Eric T. Olson
Senate Armed Services Committee
testimony, 4 Mar 08

Near-Term Actions

a. Create USSOCOM Instruction 25-4 and implement a USSOCOM portfolio management process in synchronization with DoD governing guidance that provides the command a standard process for the selection and management of IT investments to maximize SOF capabilities.

b. Implement an automated SOF IT portfolio management system to provide the USSOCOM Chief Information Officer (CIO), Chief Financial Officer (CFO), and Acquisition Executive (AE) accurate visibility of SOF Information and Intelligence Systems (IIS) to better enable effective IT investment decisions for operational requirements.

c. Publish guidance to provide the headquarters, components, and SOF commanders at all levels instructions for the Program Objective Memorandum (POM), Program Review (PR) process to synchronize our budget development efforts for SOF IT resources.

d. Utilize the SOF IT portfolio management system to develop and provide SOF Information and Intelligence Systems (IIS) inputs to the POM/PR development process.

e. Deliver an action plan to utilize the SOF IT portfolio management system to validate and develop the following annual DoD requirements for the CIO: IT Systems Registration and Certification of Compliance; DoD Component Data Traceability; IT Budget Submission and Statement of Compliance.

Strategic Actions

a. Expand the SOF IT portfolio management system to include all information and IT investments throughout USSOCOM.

b. Develop an action plan to ensure data compliance and validation in the SOF IT portfolio management system.
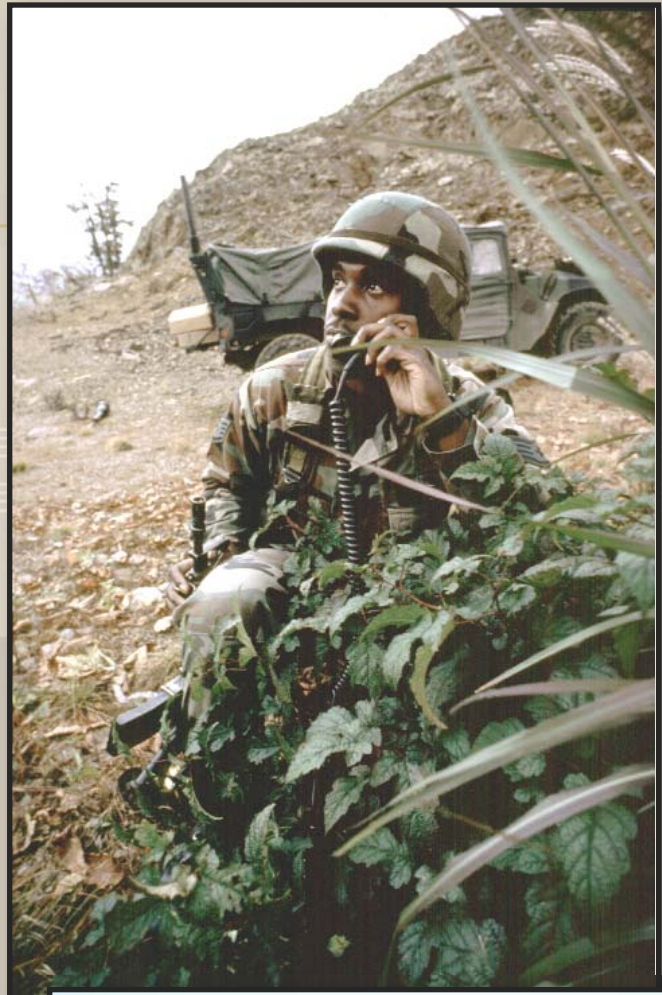
IV. SUMMARY

The SOF Information Environment is one of USSOCOM's many success stories. It has been and continues to be an instrumental tool in SOF's efforts fighting the Global War on Terror. With my vision of One Force, One Environment, I intend to reinforce those successes with state of the art, leap-ahead technological innovations, with transformational business process solutions, and through efficient management of the precious resources entrusted to USSOCOM.